What is claimed is:

1. A digital information protecting method for encrypting a piece of digital information from an author computer with assistances from a server, and then transmitting an encrypted digital information to a client computer via a computer network for the client computer to decrypt the encrypted digital information to be used, both the author computer and the client computer comprising a predetermined information processing software to process the piece of digital information, the method comprising:

in the author computer:

receiving a content key from a server and encrypting the piece of digital information by the content key;

encrypting the content key by a predetermined key encrypting process; and

transmitting the encrypted digital information and the encrypted content key to the client computer; and

in the client computer:

decrypting the encrypted content key by a corresponding predetermined key decrypting process; and

decrypting the encrypted digital information by the content key to make the piece of digital information can be used by the client computer.

2. The digital information protecting method of claim 1, wherein the author computer draws up a policy relating to the piece of digital information, and transmits the policy to the server.

3. The digital information protecting method of claim 2, wherein the policy comprises the range, time, and using times of the piece of digital information being authorized.

4. The digital information protecting method of claim 1, wherein the information processing software of the author computer comprises a plurality of universal keys with encoded serial number.

5. The digital information protecting method of claim 4, wherein the key encrypting process is executed the following steps by the information processing software of the author computer:

choosing one of the plurality of universal keys, and encrypting the content key by the chosen universal key, and

storing the encrypted content key and the serial number of the universal key to a header, and adding the header in front of the encrypted digital information.

6. The digital information protecting method of claim 5, wherein before the information processing software of the author computer executes the key encrypting process, the software asks the author of the author computer to authorize an Off-line Access Permission.

7. The digital information protecting method of claim 6, wherein the Off-line Access Permission determines whether the client computer is permitted to process and use the received piece of digital information in the off-line situation.

8. The digital information protecting method of claim 7, wherein the key decrypting process is executed the following steps by the information processing software of the client computer:

getting a corresponding universal key according to serial number stored in the header; and

decrypting the content key by the universal key.

9. The digital information protecting method of claim 8, wherein the information processing software of the client computer downloads the universal key from the server according to the serial number.

10. The digital information protecting method of claim 8, wherein the information processing software of the client computer comprises a plurality of universal keys, the information processing software of the client computer chooses corresponding universal key according to the serial number.

11. The digital information protecting method of claim 1, wherein the information processing software encrypts and decrypts the piece of digital information by Advanced Encryption Standard (AES) method.

12. A digital information protecting system for encrypting a piece of digital information from an author computer with assistances from a server, and then transmitting an encrypted digital information to a client computer via a computer network for the client computer to decrypt the encrypted digital information to be used, both the author computer and the client computer comprising a predetermined

information processing software to process the piece of digital information, the system comprising:

a first digital information process software, being set in the author computer, comprising:

a content encrypting module, for

receiving a content key from a server; and

encrypting the piece of digital information by the content key; and

a key encrypting module, for

encrypting the content key by a predetermined key encrypting process; and

transmitting the encrypted digital information and the encrypted content key to the client computer; and

a second information process software, setting in the client computer, comprising:

a key decrypting module, for

decrypting the encrypted content key by a corresponding predetermined decrypting process; and

a content decrypting module, for

decrypting the encrypted digital information by the content key to make the piece of digital information can be used by the client computer.

13. The digital information protecting system of claim 14, wherein the author computer draws up a policy relating to the piece of digital information, and transmits the policy to the server.

14. The digital information protecting system of claim 15, wherein the policy comprises the range, time, and using times of the piece of digital information being authorized.

15. The digital information protecting system of claim 14, wherein the information processing software of the author computer comprises a plurality of universal keys with encoded serial number.

16. The digital information protecting system of claim 17, wherein the key encrypting process is executed the following steps by the information processing software of the author computer:

choosing one of the plurality of universal keys, and encrypting the content key by the chosen universal key, and

storing the encrypted content key and the serial number of the universal key to a header, and adding the header in front of the encrypted digital information.

17. The digital information protecting system of claim 18, wherein before the information processing software of the author computer executes the key encrypting process, the software asks the author of the author computer to authorize an Off-line Access Permission.

18. The digital information protecting system of claim 19, wherein the Off-line Access Permission determines whether the client computer is permitted to process and use the received piece of digital information in the off-line situation.

19. The digital information protecting system of claim 20, wherein the key decrypting process is executed the following steps by the information processing software of the client computer:

getting a corresponding universal key according to serial number stored in the header; and

decrypting the content key by the universal key.

20. The digital information protecting method of claim 21, wherein the information processing software of the client computer downloads the universal key from the server according to the serial number, the information processing software of the client computer chooses corresponding universal key according to the serial number.

21. The digital information protecting method of claim 21, wherein the information processing software of the client computer comprises a plurality of universal keys.

22. The digital information protecting system of claim 14, wherein the information processing software encrypts and decrypts the piece of digital information by Advanced Encryption Standard (AES) method.

23. A digital information protecting method for encrypting a piece of digital information from an author computer with assistances from a server, and then transmitting an encrypted digital information to a client computer via a computer network for decrypting the encrypted digital information to be used, the method

comprising:

in the author computer, encrypting the piece of digital information by a content key;

in the author computer, encrypting the content key by a public key;

in the author computer, transmitting the piece of encrypted digital information and the encrypted content key to the client computer;

in the client computer, receiving the piece of encrypted digital information and the encrypted content key;

in the client computer, transmitting the encrypted content key to the server;

in the server, decrypting the encrypted content key by a private key corresponding to the public key;

in the server, transmitting the decrypted content key to the client computer; and

in the client computer, decrypting the piece of encrypted digital information by the decrypted content key.

24. The digital information protecting method of claim 23, the author computer further draws up a policy relating to the piece of digital information, and transmits the policy to the server.

25. The digital information protecting method of claim 24, wherein the policy comprises the range, time, and using times of the piece of digital information being authorized.

26. The digital information protecting method of claim 23, wherein the server transmits

the public key to the author computer.

27. The digital information protecting method of claim 26, wherein the public key transmitted from the server is acquired from an issue device.

28. The digital information protecting method of claim 27, wherein the encrypted content key are stored in a header, and added the header in front of the encrypted digital information.

29. The digital information protecting method of claim 28, wherein the content key is encrypted and decrypted by Advanced Encryption Standard (AES) method.

30. The digital information protecting method of claim 29, wherein the public key and the private key are encrypted and decrypted by Rivest Shamir Adleman (RSA) method.

31. A digital information protecting system for encrypting and decrypting a piece of digital information, the system comprising:

a content encrypting module, for using a content key to encrypt the piece of digital information;

a key encrypting module, for using a public key to encrypt the content key;

a key decrypting module, for decrypting the encrypted content key by a private key corresponding to the public key; and

a content decrypting module, for decrypting the piece of encrypted digital information by the content key.

32. The digital information protecting system of claim 31, wherein the content encrypting module and the key encrypting module are set in a author computer, and the content decrypting module is set in a client computer.

33. The digital information protecting system of claim 32, wherein the key decrypting module is set in a server.

34. The digital information protecting system of claim 33, the author computer further draws up a policy relating to the piece of digital information, and transmits the policy to the server.

35. The digital information protecting system of claim 34, wherein the policy comprises the range, time, and using times of the piece of digital information being authorized.

36. The digital information protecting method of claim 31, wherein the server transmits the public key to the author computer.

37. The digital information protecting method of claim 36, wherein the public key transmitted from the server is acquired from an issue device.

38. The digital information protecting method of claim 4, wherein the encrypted content key are stored in a header, and added the header in front of the encrypted digital information.

39. The digital information protecting method of claim 1, wherein the content key is encrypted and decrypted by Advanced Encryption Standard (AES) method.

40. The digital information protecting method of claim 1, wherein the public key and the private key are encrypted and decrypted by Rivest Shamir Adleman (RSA) method.